

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 678 836 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:
14.01.1998 Bulletin 1998/03

(51) Int Cl.⁶: G07F 7/10

(21) Application number: 94105573.3

(22) Date of filing: 11.04.1994

(54) Method and means for combining and managing personal verification and message authentication encryptions for network transmission

Verfahren und Vorrichtung zur Verknüpfung und zur Anwendung von Verschlüsselungen bei der Personenüberprüfung und der Authentisierung von Meldungen bei der Übertragung in Netzwerken

Méthode et moyens pour combiner et diriger le chiffage de la vérification des personnes et des messages d'authentification lors d'une transmission sur un réseau

(84) Designated Contracting States:
DE FR GB

(43) Date of publication of application:
25.10.1995 Bulletin 1995/43

(73) Proprietor: TANDEM COMPUTERS
INCORPORATED
Cupertino, California 95014-0709 (US)

(72) Inventors:
• Atalla, Martin M.
Atherton CA 94025 (US)

• Hopkins, W. Dale
Gilroy CA 95020 (US)

(74) Representative: KUHNEN, WACKER & PARTNER
Alois-Stelnecker-Strasse 22
85354 Freising (DE)

(56) References cited:
EP-A- 0 391 261 EP-A- 0 494 796
EP-A- 0 500 245 EP-A- 0 547 975
US-A- 5 016 277 US-A- 5 101 373

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 0 678 836 B1

Description

Related Cases

The subject matter of this application is related to the subject matter disclosed in U.S. Patents 4,268,715; 4,281,215; 4,283,599; 4,288,659; 4,315,101; 4,357,529; 4,536,647 and pending application for U.S. Patent Serial No. 547,207, entitled POCKET TERMINAL, METHOD AND SYSTEM FOR SECURED BANKING TRANSACTIONS, filed October 31, 1983 by M.M. Atalla.

Background of the Invention

Conventional data encryption networks commonly encrypt a Personal Identification Number with a particular encryption key for transmission along with data messages, sequence numbers, and the like, from one location node in the data network to the next location or node in the network. There, the encrypted PIN is decrypted using the encryption key, and re-encrypted with another encryption key for transmission to the next node in the network, and so on to the final node destination in the network.

In addition, such conventional data encryption networks also develop a Message Authentication Codes in various ways, and then encrypt such MAC for transmission to the next node using a MAC-encryption key that is different from the encryption key used to encrypt the PIN. At such next node, the MAC is decrypted using the MAC encryption key and then re-encrypted using a new MAC-encryption key for transmission to the next node, and so on to the final destination node in the network.

Further, such conventional networks operate upon the PIN, MAC, data message, sequence number, and the like, received and decrypted at the final destination node to consummate a transaction, or not, and then communicate an ACKnowledgment or Non-ACKnowledgment message back to the originating node of the network. Such ACK or NACK codes may be encrypted and decrypted in the course of transmission node by node through the network back to the originating node to provide an indication there of the status of the intended transaction at the final destination node.

Conventional data encryption networks of this type are impeded from handling greater volumes of messages from end to end by the requirement for separately encrypting and decrypting the PIN and MAC codes at each node using different encryption/decryption keys for each, and by the requirement for encrypting/decrypting at least the ACK code at each node along the return path in the network.

In addition, such conventional data encryption networks are susceptible to unauthorized intrusion and compromise of the security and message authenticity from node to node because of the separated PIN and MAC encryption/decryption techniques involved. For

example, the encrypted PIN is vulnerable to being "stripped" away from the associated MAC, message, sequence number, and the like, and to being appended to a different MAC, message, sequence number, and the like, for faithful transmission over the network. Further, the return acknowledgment code may be intercepted and readily converted to a non-acknowledgment code or simply be altered in transmission after the transaction was completed at the destination node. Such a return code condition could, for example, cause the user to suffer the debiting of his account and, at the same time, the denial of completion of a credit purchase at point-of-sale terminal or other originating node.

It is known from US-Patent 5,101,373, to avoid the drawback of encryption and decryption of personal identification information and of message data information, sequence numbers, and the like, respectively when transmitting such information from one location to a next location by providing an approval operation parameter generator in a first location acting as the information transmitting location, said approval operation parameter generator generating an initial cipher value and an encipher key and sending these parameters to a second location acting as the information receiving location. Those said locations keep stored therein the same program data segmented in a first and a second plurality of data blocks, respectively. An approval calculation is carried out at both locations enciphering the respective plurality of segmented data blocks with the said parameters, the respective results of the calculation on the side of the receiving location and on the side of the transmitting location being compared within a central processing unit on the side of the transmitting location. The result of this comparison, if not satisfactory, inhibits the communication between said both locations.

From European patent application publication No. 0 391 261 a telecommunication system is known implementing a checking of double use of electronic cash issued from a bank and accepted e.g. by a shop from the user. The user generates user information from secret information containing user's identifications, and creates an authentication information. The user makes a bank apply a blind signature to the user information and to the authentication information in a one-way-function. The electronic cash receiving shop verifies the validity of the user information and the authentication information both signed by the bank. In response to a subsequent inquiry of the shop the user produces a response by removing the influence of the randomisation and of the secret information so that, after verifying the validity of the response, the shop accepts the electronic cash.

It is an object of the present invention to provide an improved method of securing transaction data between two locations in response to a user's personal identification number in the sense of increasing the security and simplifying the encoding and decoding operations.

This object, in accordance with the present invention, is achieved by a method with the features of at-

tached claim 1. Furthermore, said object is also achieved by an apparatus with the features of appended claim 5.

Accordingly, the method and means for integrating the encryption keys associated with the PIN and MAC codes according to the present invention assure that these codes are sufficiently interrelated and that alteration of one such code will adversely affect the other such code and inhibit message authentication in the network. In addition, the return acknowledgment or non-acknowledgment code may be securely returned from node to node in the network without the need for encryption and decryption at each node, and will still be securely available for proper validation as received at the originating node. This is accomplished according to the present invention by using one session key to encrypt the PIN along with the MAC, a random number, the message, and the sequence number which are also encrypted with the PIN such that re-encryption thereof in the transmission from location to location, or node to node over a network is greatly facilitated and validatable at each node, if desired. In addition, portions of the random number are selected for use as the Acknowledgment or Non-Acknowledgment return codes which can be securely returned and which can then only be used once to unambiguously validate the returned code only at the originating node in the network.

Description of the Drawings

FIG. 1 is graphic representation of a typical conventional encryption scheme which operates with two independent session keys;

FIGS. 2, 2A, 2B and 2C are schematic representations of a second network according to the present inventions; and

FIGS. 3, 3A, 3B and 3C are graphic representations of the signal processing involved in the operation of the network of FIG. 2.

Description of the Preferred Embodiment

Referring now to Figure 1, there is shown a graphic representation of the encoding scheme commonly used to produce the PIN and MAC codes using two session keys for transmission separately to the next network node. As illustrated, one session key 5 may be used to encrypt the PIN entered 7 by a user (plus a block of filler bits such as the account number, as desired) in a conventional encryption module 9 which may operate according to the Data Encryption Standard (DES) established by the American National Standards Institute (ANSI) to produce the encrypted PIN signal 11 (commonly referred to as the PIN block* according to ANSI standard 9.3) for transmission to the next network node. In addition, the message or transaction data which is entered 13 by the user and which is to be transmitted to another node, is combined with a sequence number 15

that may comprise the date, time, station code, and the like, for encryption by a DES encryption module 17 with another session key 19 to produce a Message Authentication Code (MAC) 21 for that message and sequence number. The MAC may comprise only a selected number of significant bits of the encrypted code. The message and MAC are separately transmitted to the next node along with the encrypted PIN, and these codes are separately decrypted with the respective session keys and then re-encrypted with new separate session keys for transmission to the next network node, and so on, to the destination node. Conventional PIN validation at the destination node, and message authentication procedures may be performed on the received, encrypted PIN and MAC, (not illustrated) and the message is then acted upon to complete a transaction if the PIN is valid and the MAC is unaltered. A return ACKnowledgment (or Non-ACKnowledgment) code may be encrypted and returned to the next node in the network over the return path to the originating node. At each node in the return path, the ACK code is commonly decrypted and re-encrypted for transmission to the next node in the return path, and so on (not illustrated), to the originating node where receipt of the ACK is an indication that the transaction was completed at the destination node. Conventional systems with operating characteristics similar to those described above are more fully described, for example, in U.S. Patent 4,283,599.

One disadvantage associated with such conventional systems is the need to encrypt and decrypt at each node using two separate session keys. Another disadvantage is that such conventional systems are vulnerable to unauthorized manipulation at a network node by which the message and MAC may be "stripped away" from the encrypted PIN associated with such message and replaced with a new message and MAC for transmission with the same encrypted PIN to the next network node. Further, the acknowledgement code that is to be returned to the originating node not only must be decrypted and re-encrypted at each node along the return path, but the return of an acknowledgment code that is altered along the return path may connote non-acknowledgment or non-completion of the intended transaction at the destination node. This condition can result in the account of the user being debited (the PIN and MAC were valid and authentic as received at the destination node), but the user being denied completion of a credit transaction (e.g., transfer of goods) at the originating node.

Referring now to Figures 2 and 3, there are shown schematic and graphic representations, respectively, of network operations according to the present invention. Specifically, there is shown a system for transmitting a message over a network 29 from an originating node 31 to a destination node 33 via an intermediate node 35. At the originating node 31, an authorized user enters his PIN 37 of arbitrary bit length with the aid of a key board,

or card reader, or the like, and the entered PIN is then filled or blocked 39 with additional data bits (such as the user's account number in accordance with ANSI standard 9.3) to configure a PIN of standard bit length.

In addition, the transaction data or message 41 entered through a keyboard, or the like, by the user is combined with a sequence number 43 which is generated to include date, time of day, and the like. The combined message and sequence number is encrypted 45 with the PIN (or blocked PIN) in a conventional DES module to produce a multi-bit encrypted output having selected fields of bits, one field of which 53 serves as the Message Authentication Code (MAC). Other schemes may also be used to produce a MAC, provided the PIN (or blocked PIN) is used as the encryption key, and the resulting MAC, typically of 64-bit length, may be segregated into several sectors or fields 51. A random number (R/N) is generated 52 by conventional means and is segregated into several sectors or fields 54, 56, 58. The first sector or field 54 of, say 32-bits length, is then encrypted with the selected MAC field 53 in a conventional DES encryption module 55 (or in DES module 45 in time share operation) using the session key K_1 as the encryption key 50. In addition, the PIN (or blocked PIN) 39 is encrypted in DES encryption module 60 (or in DES module 45 in time share operation) using the session key K_1 as the encryption Key 50. The session key 50 may be transmitted to successive nodes 35, 33 in secured manner, for example, as disclosed in U.S. Patent 4,288,659. The resulting encrypted output codes 62, 64 are then transmitted along with sequence number 43 and the message 41 (in clear or cypher text) over the network 29 to the next node 35 in the path toward the destination node 33. Thus, only a single session key K_1 is used to encrypt the requisite data for transmission over the network, and the residual sectors or fields 56, 58 of the random number from generator 52 remain available to verify successful completion of the transaction at the destination node 33, as later described herein.

At the intermediate node 35, the encrypted PIN 64 received from the originating node 31 is decrypted in conventional DES module 70 using the session key K_1 to produce the blocked PIN 63. In addition, the encrypted MAC and R/N 68 received from the originating node is decrypted in conventional DES module 61 (or in DES module 70 operating in timeshare relationship) using session key K_1 to produce the MAC and the R/N in segregated fields. An initial validation may be performed by encrypting the received message 41 and sequence number 43 in conventional DES module 67 using the decrypted PIN 63 as the encryption key. Of course, the original PIN as entered by the user may be extracted from the decrypted, blocked PIN 63 to use as the encryption key in module 67 if the corresponding scheme was used in node 31. (It should be understood that the PIN or blocked PIN does not appear in clear text outside of such decryption or encryption modules 70, 67 (or 69,

later described herein), and that these modules may be the same DES module operated in time-shared relationship.)

The encrypted output of module 67 includes several sectors, or fields, similar to those previously described in connection with the encrypted output of module 45. The selected sector 53 of significant bits that constitutes the MAC is selected for comparison with the MAC 65 that is decrypted in DES module 61. This decryption also provides the R/N having several selected sectors or fields 72. If the comparison of the decrypted and encrypted MAC's in comparator 74 is favorable, gate 76 is enabled and the decrypted MAC and R/N are encrypted in conventional DES module 69 using new session key K_2 as the encryption key, and gate 88 is enabled to encrypt the decrypted PIN in DES module 78 (or in DES module 67 or 69 in time share operating). If comparison is unfavorable, the transaction may be aborted and the gate 80 is enabled to transmit back to the originating node 31 the sector or field 58 of the R/N which constitutes the Non ACKnowledge sector of the decrypted R/N output of module 61. The encrypted PIN output 82 of module 78 and the encrypted MAC and R/N output 84 of the module 69 are thus transmitted along with the message 41 and sequence number 43 over the network 29 to the destination node 35 upon favorable comparison 74 of the encrypted and decrypted MACs.

At the destination node 33, the encrypted PIN output 86 received from the intermediate node 35 is decrypted in conventional DES module 71 using the session key K_2 to produce the PIN 73. An initial validation may be performed by encrypting the received message 41 and sequence number 43 in conventional DES module 77, using the decrypted PIN 73 as the encryption key. As was described in connection with the intermediate node 35, the original PIN as entered by the user may be extracted from the decrypted, blocked PIN 73 to use as the encryption Key in module 77 if the corresponding scheme was used in node 31. And, it should be understood that the PIN or blocked PIN does not appear in clear text outside of the decryption or encryption modules 71, 77, which modules may be the same DES module operated in time-shared relationship. In addition, the encrypted MAC and R/N received at the destination node 33 is decrypted in DES module 92 using the session key K_2 to produce the MAC 75 and the R/N 94 in segregated sectors or fields. The selected sector 53 of significant bits that constitutes the MAC in the encrypted output of module 77 is compared 79 for parity with the decrypted MAC 75. If comparison is favorable, the transaction may be completed in response to the message 41, and gate 81 may be enabled to transmit 29 back to the intermediate node 35 a second selected sector or field 56 which constitutes the ACKnowledge output sector of the R/N decrypted output from module 92. If comparison 79 is unfavorable, the transaction is not completed and gate 83 is enabled to transmit 29 back to the intermediate node 35 a third selected sector or field 58

which constitutes the Non-ACKnowledge sector of the R/N decrypted output from module 92.

In accordance with one aspect of the present invention, the returned ACK or NACK codes do not require decryption and re-encryption when transmitted from node to node along the return path in the network back to the originating node 31. Instead, these codes are already in encoded form and may be transmitted directly from node to node without encumbering a node with additional operational overhead. These codes are therefore secured in transmission over the network and are only cypherable in the originating node 31 which contains the ACK and NACK fields or sectors 56 and 58 of the random number from generator 52. At the originating node 31, the second and third sectors or fields 56 and 58 of the random number are compared 98 with the corresponding sectors of decrypted R/N outputs received from the destination node 33 (or the sector 58 of the decrypted R/N output received from intermediate node 35) to provide an indication at the originating node that the transaction was either completed 89 or aborted 91. Of course, the ACK and NACK may be encrypted as a network option when returned to the originating node 31. And, it should be understood that the encryption and decryption modules at each node may be the same conventional DES module operated in timeshare relationship.

Therefore, the system and method of combining the management of PIN and MAC codes and the session keys associated therewith from node to node along a data communication network obviates the conventional need for separate session keys for the PIN and the MAC, and also obviates the need for conventional encryption/decryption schemes for an acknowledgment code at each node along the return path back to the originating node. If desired, PIN validations may be performed at each node since the PIN is available within the DES module circuitry. In addition, the present system and method also reduces the vulnerability of a secured transmission system to unauthorized separation of a valid PIN code from its associated message and MAC code for unauthorized attachment to a different message and MAC code. Further, the method and means of the present invention reduces the ambiguity associated with the return or not of only an acknowledgment code in conventional systems by returning either one of the ACK and NACK codes without additional operational overhead at each node.

Claims

1. The method of securing transaction data between two locations in response to a user's message and personal identification number, the method comprising:

forming a sequence number representative of

the user's transaction;
 encoding in a first logical combination at the first location the user's message and the sequence number in accordance with the personal identification number received from the user to produce a message authentication code having a plural number of digit sectors;
 generating a random number;
 establishing a first encoding key;
 encoding in a second logical combination at the first location the random number and a selected number of sectors of the message authentication code in accordance with the first encryption key to produce a first coded output;
 encoding in a third logical combination at the first location the user's personal identification number in accordance with the first encoding key to produce a second coded output;
 transmitting to another location the user's message and the sequence number and the first and second coded outputs;
 establishing the first encoding key at such other location;
 decoding the first coded output received at such other location with the first encoding key according to said second logical combination thereof to provide the random number and message authentication code;
 decoding the second coded output received at such other location with the first encoding key according to said third logical combination to provide the user's personal identification number;
 encoding in the first logical combination at such other location the user's message and sequence number received thereat in accordance with the decoded personal identification number to produce a message authentication code having a plural number of digit sectors;
 and
 comparing selected corresponding digit sectors of the decoded message authentication code and the encoded message authentication code to provide an indication upon favorable comparison of the valid transmission of the user's message between the two locations.

2. The method according to claim 1 comprising the steps of:

establishing a second encoding key at the other location;
 encoding in a fourth logical combination at such other location the decoded random number and selected sector of the message authentication code in accordance with the second encoding key to produce a third coded output;
 encoding in a fifth logical combination at the

other location the decoded user's personal identification number in accordance with the second encoding key to produce a fourth coded output;

transmitting to a remote location the user's message and the sequence number and the third and fourth coded outputs;

establishing the second encoding key at the remote location;

decoding the third coded output as received at the remote location according to the fourth logical combination in accordance with the second encoding key to provide the random number and the message authentication code having a plural number of digit sectors;

decoding the fourth coded output received at the remote location according to the fifth logical combination to provide the user's personal identification number;

encoding the message and the sequence number received at the remote location according to the first logical combination in accordance with the decoded personal identification number to produce a message authentication code having a plural number of digit sectors; and

comparing corresponding digit sectors of the decoded message authentication code and the encoded message authentication code at the remote location to provide an indication upon favorable comparison of the unaltered transmission of the message, or an indication upon unfavorable comparison of an alteration in the transmission of the message.

3. The method according to claim 1 comprising the steps of:

transmitting a selected sector of the decoded random number from the other location to the one location in response to unfavorable comparison; and

comparing the selected sector of the random number received at the one location from the other location with the corresponding selected sector at the one location to provide an indication of the altered transmission of the message to the other location.

4. The method according to claim 2 comprising the steps of:

completing the transaction and returning a second selected sector of the decoded random number from the remote location to the one location in response to said favorable comparison, and inhibiting completion of the transaction and returning a third selected sector of the

decoded random number from the remote location to the one location in response to said unfavorable comparison; and

comparing the selected sector of the random number received at the one location from the remote location with the corresponding selected sector of the number generated at the one location to provide an indication of the completion or non-completion of the transaction at the remote location.

5. Apparatus for securing transaction data between two locations (31, 35) in response to a user's message (41) and personal identification number (37), the apparatus comprising:

means for generating a sequence number associated with a user's transaction;

means (52) for generating a random number; first encryption means (45) at one location for encrypting according to a first logical combination of the user's message and the sequence number applied thereto with the personal identification number received from the user for producing a message authentication code therefrom having a plural number of digit sectors;

means (50) at said one location for producing a first session key;

second encryption means (55) coupled to receive the random number from the user and a selected sector of the message authentication code for encrypting the same with the first session key according to a second logical combination thereof to produce a first encoded output (62);

third encryption means (60) coupled to receive the personal identification number from the user for encrypting the same with the first session key according to a third logical combination thereof to produce a second encoded output (64);

means (29) for transmitting the first and second encoded outputs and message and sequence number from the one location to the next location;

means at the next location for producing the first session key (session key₁);

first decryption means (61) at the next location coupled to receive the transmitted first encoded output (68) and the first session key for decrypting in accordance with said second logical combination to provide the random number and the message authentication code (65);

second decryption means (70) at the next location coupled to receive the transmitted second encoded output and the first session key for decrypting in accordance with the third logical combination thereof to produce the user's per-

sonal identification number (63);
 third encryption means (67) at the next location
 coupled to receive the transmitted message
 and sequence number for encoding the same
 according to said first logical combination with
 the decrypted personal identification number
 (63) to produce a message authentication code
 having a plural number of digit sectors;
 comparison means (74) at the next location
 coupled to receive the corresponding selected
 sectors of the message authentication code
 (65) formed by decryption of said first decryption
 means (61) and of the message authentication
 code formed by encryption of said third encryp-
 tion means (67) at said next location for produc-
 ing an output indication of the parity thereof;
 and
 means (76) at the next location responsive to
 said output indication for operating upon the re-
 ceived message in response to favorable com-
 parison.

6. Apparatus as in claim 5 comprising:

means (80) at the next location responsive to
 the unfavorable comparison for transmitting to the
 one location a selected sector (58) of the random
 number.

7. Apparatus as in claim 5 comprising:

means at the next location for producing a sec-
 ond encoding key (session key₂);
 first encryption means (69) at the next location
 coupled to receive the decrypted message au-
 thentication code and random number for en-
 coding the same with the second encoding key
 in accordance with a fourth logical combination
 in response to said favorable comparison for
 producing a third output code for transmission
 to a destination location;
 second encryption means (78) at the next loca-
 tion coupled to receive the decrypted personal
 identification number for encoding the same
 with the second encoding key in accordance
 with a fifth logical combination in response to
 said favorable comparison for producing a
 fourth output code (82) for transmission to a
 destination location;
 means at the destination location for producing
 the second encoding key (session key₂);
 first decryption means (92) at the destination
 location for receiving the third output code (90)
 transmitted from said next location and the sec-
 ond encoding key for decoding the same ac-
 cording to said fourth logical combination to
 provide the random number (94) and the mes-
 sage authentication code (75);
 second decryption means (71) at the destina-

tion location for receiving the fourth output code
 transmitted from said next location and the sec-
 ond encoding key (session key₂) for decoding
 the same according to said fifth logical combi-
 nation to provide the personal identification
 number;

encryption means (77) at the destination loca-
 tion for receiving the message and the se-
 quence number for encoding the same with the
 decrypted personal identification number in ac-
 cordance with the first logical combination to
 produce a message authentication code having
 a plural number of digit sectors;

means (79) at the destination location for com-
 paring corresponding selected sectors of the
 encrypted message authentication code and the
 decrypted message authentication code (75) to
 produce output indications of favorable
 and unfavorable comparisons;

means (81) at the destination location respon-
 sive to favorable output indication for operating
 upon the transmitted message and for transmit-
 ting a selected sector of the random number to
 said one location, and responsive (83) to unfa-
 vorable comparison for transmitting another se-
 lected sector of the random number to said one
 location; and

comparator means (98) at the one location cou-
 pled to receive the corresponding selected sec-
 tors of the random number for providing an out-
 put indication (89, 91) of the status of operation
 upon the message at the destination location.

35 Patentansprüche

1. Verfahren zur Sicherung der Transaktion von Daten
 zwischen zwei Orten in Abhängigkeit von einer Be-
 nutzernachricht und einer persönlichen Identifizie-
 rungsnummer, wobei das Verfahren folgendes um-
 faßt:

Bilden einer Folgenummer entsprechend der
 Transaktion durch den Benutzer;

Kodieren einer ersten logischen Kombination
 der Benutzernachricht und der Folgenummer
 an einem ersten Ort entsprechend der persön-
 lichen Identifizierungsnummer, welche von
 dem Benutzer empfangen worden ist, um einen
 Nachrichten-Berechtigungskode zu erzeugen,
 welcher eine Mehrzahl von digitalen Sektoren
 aufweist;

Erzeugen einer Zufallszahl;

Festsetzen eines ersten Kodierungsschlüs-
 sels;

- Kodieren einer zweiten logischen Kombination der Zufallszahl und einer gewählten Zahl von Sektoren des Nachrichten-Berechtigungskodes an dem ersten Ort entsprechend dem ersten Verschlüsselungskode zur Erzeugung eines ersten kodierten Ausgangs; 5
- Kodieren einer dritten logischen Kombination der persönlichen Identifizierungsnummer des Benutzers an dem ersten Ort entsprechend dem ersten Kodierungsschlüssel zur Erzeugung eines zweiten kodierten Ausgangs; 10
- Übertragen der Benutzernachricht und der Folgenummer sowie des ersten und zweiten kodierten Ausgangs zu einem anderen Ort; 15
- Festsetzen des ersten Kodierungsschlüssels an diesem genannten anderen Ort; 20
- Dekodieren des ersten kodierten Ausgangs, welcher an diesem anderen Ort empfangen wird, unter Verwendung des ersten Kodierungsschlüssels entsprechend der genannten zweiten logischen Kombination zur Erzeugung der Zufallszahl und des Nachrichten-Berechtigungskodes; 25
- Dekodieren des zweiten kodierten Ausgangs, welcher an diesem anderen Ort empfangen wird, unter Verwendung des ersten Kodierungsschlüssels entsprechend der genannten dritten logischen Kombination zur Erzeugung der persönlichen Identifizierungsnummer des Benutzers; 30 35
- Kodieren gemäß der ersten logischen Kombination an dem genannten anderen Ort, der Benutzernachricht und der Folgenummer, welche dort empfangen worden sind, entsprechend der dekodierten persönlichen Identifizierungsnummer, um einen Nachrichten-Berechtigungskode zu erzeugen, der eine Mehrzahl von digitalen Sektoren aufweist; und 40 45
- Vergleichen ausgewählter entsprechender Digitalektoren des dekodierten Nachrichten-Berechtigungskodes und des kodierten Nachrichten-Berechtigungskodes zur Erzeugung einer Anzeige bezüglich eines positiven Vergleiches der gültigen Übertragung der Benutzernachricht zwischen zwei Orten. 50
2. Verfahren nach Anspruch 1, enthaltend die folgenden Schritte: 55
- Festsetzen eines zweiten Kodierungsschlüssels an dem genannten anderen Ort;
- Kodierung gemäß einer vierten logischen Kombination an dem genannten anderen Ort von der dekodierten Zufallszahl und dem gewählten Sektor des Nachrichten-Berechtigungskodes entsprechend dem zweiten Kodierungsschlüssel zur Erzeugung eines dritten kodierten Ausgangs;
- Kodierung gemäß einer fünften logischen Kombination an dem anderen Ort von der dekodierten persönlichen Benutzeridentifizierungsnummer entsprechend dem zweiten Kodierungsschlüssel zur Erzeugung eines vierten kodierten Ausgangs;
- Übertragen der Benutzernachricht und der Folgenummer sowie des dritten und vierten kodierten Ausgangs an einen entfernten Ort;
- Festsetzen eines zweiten Kodierungsschlüssels an dem entfernten Ort;
- Dekodieren des dritten kodierten Ausgangs entsprechend dem Empfang an dem genannten entfernten Ort entsprechend der vierten logischen Kombination nach dem zweiten Kodierungsschlüssel zur Erzeugung der Zufallszahl und des Nachrichten-Berechtigungskodes mit einer Mehrzahl von digitalen Sektoren;
- Dekodieren des vierten kodierten Ausgangs, wie er an dem entfernten Ort empfangen worden ist, entsprechend der fünften logischen Kombination zur Erzeugung der persönlichen Identifizierungsnummer des Benutzers;
- Kodieren der Nachricht und der Folgenummer, wie sie an dem entfernten Ort empfangen worden sind, entsprechend der ersten logischen Kombination gemäß der dekodierten persönlichen Identifizierungsnummer zur Erzeugung eines Nachrichtenberechtigungskodes mit einer Mehrzahl von digitalen Sektoren; und
- Vergleichen entsprechender digitaler Sektoren des dekodierten Nachrichten-Berechtigungskodes und des kodierten Nachrichten-Berechtigungskodes an dem entfernten Ort zur Erzeugung einer Anzeige bezüglich eines zutreffenden Vergleiches der ungeänderten Übertragung der Nachricht oder der Anzeige eines negativen Vergleiches einer Änderung der Übertragung der Nachricht.
3. Verfahren gemäß Anspruch 1, umfassend die folgenden Schritte:
- Übertragung eines ausgewählten Sektors der

dekodierten Zufallszahl von dem anderen Ort zu dem genannten einen Ort entsprechend einem negativen Vergleich; und

Vergleichen des ausgewählten Sektors der Zufallszahl, wie sie an dem einen Ort von dem anderen Ort empfangen wurde, mit dem entsprechenden ausgewählten Sektor an dem einen Ort, zur Erzeugung einer Anzeige einer geänderten Übertragung der Nachricht zu dem anderen Ort.

4. Verfahren nach Anspruch 2, umfassend die folgenden Schritte:

Vervollständigen der Transaktion und Rückgabe eines zweiten ausgewählten Sektors der dekodierten Zufallszahl von dem entfernten Ort zu dem einen Ort in Abhängigkeit von dem genannten positiven Vergleich, und Verhindern der Vervollständigung der Transaktion und Rückgabe eines dritten ausgewählten Sektors der dekodierten Zufallszahl von dem entfernten Ort zu dem genannten einen Ort in Abhängigkeit von einem negativen Vergleich; sowie

Vergleichen des ausgewählten Sektors der Zufallszahl, wie sie an dem genannten einen Ort von dem entfernten Ort empfangen worden ist, mit dem entsprechenden ausgewählten Sektor der Zahl, die an dem einen Ort erzeugt wurde, um eine Anzeige der Vervollständigung oder Nicht-Vervollständigung der Transaktion an dem entfernten Ort zu erzeugen.

5. Einrichtung zur Sicherung einer Datentransaktion zwischen zwei Orten (31, 35) entsprechend einer Benutzernachricht (41) und einer persönlichen Identifizierungsnummer (37), wobei die Einrichtung folgendes enthält:

Mittel zur Erzeugung einer Folgenummer, welcher einer Benutzertransaktion zugeordnet ist;

Mittel (52) zur Erzeugung einer Zufallszahl;

erste Verschlüsselungsmittel (45) an einem Ort zur Verschlüsselung, gemäß einer ersten logischen Kombination, der Benutzernachricht und der Folgenummer, welche dort zugeführt werden, mit der persönlichen Identifizierungsnummer, welche von dem Benutzer empfangen wurde, zur Erzeugung eines Nachrichten-Berechtigungskodes von dort mit einer Mehrzahl von Digitalsektoren;

Mittel (50) an dem genannten einen Ort zur Erzeugung eines ersten Bearbeitungsschlüssels;

zweite Verschlüsselungsmittel (55), welche so beschaltet sind, daß sie die Zufallszahl von dem Benutzer und einem ausgewählten Sektor des Nachrichten-Berechtigungskodes empfangen, um dieselben mit dem ersten Bearbeitungsschlüssel entsprechend einer zweiten logischen Kombination davon zu verschlüsseln, um einen ersten verschlüsselten Ausgang zu erzeugen (62);

dritte Verschlüsselungsmittel (60), welche so beschaltet sind, daß sie die persönliche Identifizierungsnummer von dem Benutzer empfangen, um dieselbe mit dem ersten Bearbeitungsschlüssel entsprechend einer dritten logischen Kombination davon zu verschlüsseln, um einen zweiten kodierten Ausgang (64) zu erzeugen;

Mittel (29) zur Übertragung des ersten und des zweiten kodierten Ausganges und der Nachricht sowie der Folgezahl von dem einen Ort zu dem nächsten Ort;

Mittel, welche an dem nächsten Ort vorgesehen sind, zur Erzeugung des ersten Bearbeitungsschlüssels (session key₁);

erste Entschlüsselungsmittel (61) an dem nächsten Ort, welche so beschaltet sind, daß sie den übertragenen ersten kodierten Ausgang (68) und den ersten Bearbeitungsschlüssel empfangen, um eine Entschlüsselung entsprechend der zweiten logischen Kombination vorzunehmen, um die Zufallszahl und den Nachrichten-Berechtigungskode (65) zu erzeugen;

zweite Entschlüsselungsmittel (70) an dem nächsten Ort, welche so beschaltet sind, daß sie den übertragenen zweiten kodierten Ausgang und den ersten Bearbeitungsschlüssel empfangen, um eine Entschlüsselung entsprechend der dritten logischen Kombination davon vorzunehmen, um die persönliche Identifizierungsnummer des Benutzers (63) zu erzeugen;

dritte Verschlüsselungsmittel (67) an dem nächsten Ort, welche so beschaltet sind, daß sie die übertragene Nachricht und die Folgenummer empfangen, um dieselben entsprechend der genannten ersten logischen Kombination mit der entschlüsselten persönlichen Identifizierungsnummer (63) zu kodieren, um einen Nachrichten-Berechtigungskode mit einer Mehrzahl von Digitalsektoren zu erzeugen;

Vergleichsmittel (74) an dem nächsten Ort, welche so beschaltet sind, daß sie die entspre-

chenden ausgewählten Sektoren des Nachrichten-Berechtigungskodes (65) empfangen, welche durch Entschlüsselung der genannten ersten Entschlüsselungsmittel (61) und des Nachrichtenberechtigungskodes erzeugt sind, der durch Verschlüsselung der dritten Verschlüsselungsmittel (67) an dem genannten nächsten Ort gebildet ist, um eine Ausgangsanzeige der Gleichwertigkeit von diesen zu erzeugen; und

Mittel (76) an dem nächsten Ort, welche auf die genannte Ausgangsanzeige ansprechen, um auf die empfangene Nachricht entsprechend einem zutreffenden Vergleich zu reagieren.

6. Einrichtung nach Anspruch 5, enthaltend:
Mittel (80) an dem nächsten Ort, welche auf den negativen Vergleich ansprechen, um an den genannten einen Ort einen ausgewählten Sektor (58) der Zufallszahl zu übertragen.

7. Einrichtung nach Anspruch 5, enthaltend:

Mittel, welche an dem nächsten Ort angeordnet sind, um einen zweiten Bearbeitungsschlüssel (session key₂) zu erzeugen;

erste Verschlüsselungsmittel (69) an dem nächsten Ort, welche so beschaltet sind, daß sie den entschlüsselten Nachrichten-Berechtigungskode und eine Zufallszahl empfangen, um dieselben mit dem zweiten Verschlüsselungskode entsprechend einer vierten logischen Kombination gemäß dem genannten positiven Vergleich zu kodieren, um einen dritten Ausgangskode zur Übertragung zu einem Bestimmungsort zu erzeugen;

zweite Verschlüsselungsmittel (78) an dem nächsten Ort, welche so beschaltet sind, daß sie die persönliche entschlüsselte Identifikationsnummer empfangen, um dieselbe mit dem zweiten Kodierungsschlüssel gemäß einer fünften logischen Kombination in Abhängigkeit von dem genannten positiven Vergleich zu kodieren, um einen vierten Ausgangskode (82) zur Übertragung an einen Bestimmungsort zu erzeugen;

an dem Bestimmungsort angeordnete Mittel zur Erzeugung des genannten zweiten Kodierungsschlüssels (session key₂);

erste Entschlüsselungsmittel (92), welche an dem Bestimmungsort angeordnet sind, um den dritten Ausgangskode (90), der von dem nächsten Ort übertragen wird, sowie den zweiten

Kodierungsschlüssel zur Dekodierung desselben entsprechend der genannten vierten logischen Kombination zur Erzeugung der Zufallszahl (94) und des Nachrichten-Berechtigungskodes (75) zu empfangen;

zweite Entschlüsselungsmittel (71), welche an dem Bestimmungsort angeordnet sind, zum Empfang des vierten Ausgangskodes, der von dem genannten nächsten Ort übertragen worden ist, sowie des zweiten Kodierungsschlüssels (session key₂) zur Dekodierung desselben entsprechend der genannten fünften logischen Kombination zur Erzeugung der persönlichen Identifikationsnummer;

Verschlüsselungsmittel (77), welche an dem Bestimmungsort angeordnet sind, zum Empfang der Nachricht und der Folgezahl zur Kodierung derselben mit der entschlüsselten persönlichen Identifikationsnummer gemäß der fünften logischen Kombination zur Erzeugung eines Nachrichten-Berechtigungskodes mit einer Mehrzahl von Digitalsektoren;

Mittel (79) an dem Bestimmungsort zum Vergleichen entsprechender ausgewählter Sektoren des verschlüsselten Nachrichten-Berechtigungskodes und des entschlüsselten Nachrichten-Berechtigungskodes (75) zur Erzeugung von Ausgangsanzeigen eines zutreffenden oder negativen Vergleiches;

Mittel (81) an dem Bestimmungsort, welche auf die Ausgangsanzeige des zutreffenden Vergleiches ansprechen, um bei Empfang der übertragenen Nachricht zu reagieren und einen ausgewählten Sektor der Zufallszahl zu dem genannten einen Ort zu übertragen und um in Abhängigkeit (83) eines negativen Vergleiches einen anderen ausgewählten Sektor der Zufallszahl zu dem genannten einen Ort zu übertragen; und

Vergleichsmittel (98), welche an dem genannten einen Ort angeordnet sind, welche so beschaltet sind, daß sie die entsprechenden ausgewählten Sektoren der Zufallszahl empfangen, um eine Ausgangsanzeige (89, 91) des Betriebszustandes zu liefern, sobald die Nachricht am Bestimmungsort eingetroffen ist.

Revendications

1. Procédé de sécurisation des données de transaction entre deux emplacements en réponse à un message d'utilisateur et à un numéro d'identifica-

tion personnel, le procédé comprenant :

l'élaboration d'un numéro de séquence représentatif de la transaction de l'utilisateur, le codage d'une première combinaison logique au niveau du premier emplacement, du message de l'utilisateur et du numéro de séquence conformément au numéro d'identification personnel reçu depuis l'utilisateur afin de produire un code d'authentification de message comportant un nombre multiple de secteurs de chiffres, la génération d'un nombre aléatoire, l'établissement d'une première clé de codage, le codage en une seconde combinaison logique au niveau du premier emplacement, du nombre aléatoire et d'un nombre sélectionné de secteurs du code d'authentification de message conformément à la première clé de cryptage, afin de produire une première sortie codée, le codage en une troisième combinaison logique au niveau du premier emplacement, du numéro d'identification personnel de l'utilisateur conformément à la première clé de codage afin de produire une sortie codée, la transmission vers un autre emplacement du message de l'utilisateur et du numéro de séquence et des première et seconde sorties codées, l'établissement de la première clé de codage au niveau d'un tel autre emplacement, le décodage de la première sortie codée reçue au niveau d'un tel autre emplacement, avec la première clé de codage conformément à ladite seconde combinaison logique de celui-ci afin de procurer le nombre aléatoire et le code d'authentification de message, le décodage de la seconde sortie codée reçue au niveau d'un tel autre emplacement, avec la première clé de codage conformément à ladite troisième combinaison logique afin de procurer le numéro d'identification personnel de l'utilisateur, le codage en la première combinaison logique au niveau d'un tel autre emplacement, du message de l'utilisateur et du numéro de séquence reçus au niveau de celui-ci, conformément au numéro d'identification personnel décodé afin de produire un code d'authentification de message comportant un nombre multiple de secteurs de chiffres, et la comparaison des secteurs de chiffres correspondants sélectionnés du code d'authentification de message décodé et du code d'authentification de message codé afin de procurer une indication de comparaison favorable de la transmission valide du message de l'utilisateur

entre les deux emplacements.

2. Procédé selon la revendication 1, comprenant les étapes consistant à :

établir une seconde clé de codage au niveau de l'autre emplacement, coder en une quatrième combinaison logique au niveau d'un tel autre emplacement, le nombre aléatoire décodé et le secteur sélectionné du code d'authentification de message conformément à la seconde clé de codage afin de produire une troisième sortie codée, coder en une cinquième combinaison logique au niveau de l'autre emplacement, le numéro d'identification personnel de l'utilisateur décodé conformément à la seconde clé de codage afin de produire une quatrième sortie codée, transmettre vers un emplacement à distance le message de l'utilisateur et le numéro de séquence et ainsi que les troisième et quatrième sorties codées, établir la seconde clé de codage au niveau de l'emplacement à distance, décoder la troisième sortie codée telle qu'elle est reçue au niveau de l'emplacement à distance conformément à la quatrième combinaison logique en fonction de la seconde clé de codage afin de procurer le nombre aléatoire et le code d'authentification de message comportant un nombre multiple de secteurs de chiffres, décoder la quatrième sortie codée reçue au niveau de l'emplacement à distance conformément à la cinquième combinaison logique afin de procurer le numéro d'identification personnel de l'utilisateur, coder le message et le numéro de séquence reçus au niveau de l'emplacement à distance, conformément à la première combinaison logique suivant le numéro d'identification personnel décodé afin de produire un code d'authentification de message comportant un nombre multiple de secteurs de chiffres, et comparer les secteurs de chiffres correspondants du code d'authentification de message décodé et du code d'authentification de message codé au niveau de l'emplacement à distance, afin de procurer une indication de la comparaison favorable de la transmission sans modification du message, ou bien une indication de la comparaison défavorable correspondant à une modification dans la transmission du message.

3. Procédé selon la revendication 1, comprenant les étapes consistant à :

transmettre un secteur sélectionné du nombre

aléatoire décodé depuis l'autre emplacement jusqu'au premier emplacement en réponse à une comparaison défavorable, et comparer le secteur sélectionné du nombre aléatoire reçu au niveau du premier emplacement depuis l'autre emplacement, au secteur sélectionné correspondant au niveau du premier emplacement afin de procurer une indication de la transmission modifiée du message vers l'autre emplacement.

4. Procédé selon la revendication 2, comprenant les étapes consistant à :

exécuter la transaction et renvoyer un second secteur sélectionné du nombre aléatoire décodé depuis l'emplacement à distance vers le premier emplacement, en réponse à ladite comparaison favorable, et inhiber l'exécution de la transaction et renvoyer un troisième secteur sélectionné du nombre aléatoire décodé depuis l'emplacement à distance vers le premier emplacement, en réponse à ladite comparaison défavorable, et
comparer le secteur sélectionné du nombre aléatoire reçu au niveau du premier emplacement depuis l'emplacement à distance, au secteur sélectionné correspondant du numéro généré au niveau du premier emplacement, afin de procurer une indication de l'exécution ou de la non-exécution de la transaction au niveau de l'emplacement à distance.

5. Dispositif destiné à sécuriser des données de transaction entre deux emplacements (31, 35) en réponse à un message (41) et à un numéro d'identification personnel (37) de l'utilisateur, le dispositif comprenant :

un moyen destiné à générer un numéro de séquence associé à une transaction de l'utilisateur,
un moyen (52) destiné à générer un nombre aléatoire,
un premier moyen de cryptage (45) au niveau d'un premier emplacement, afin de crypter conformément à une première combinaison logique le message et le numéro de séquence de l'utilisateur qui lui sont appliqués, ainsi que le numéro d'identification personnel reçu de l'utilisateur afin de produire un code d'authentification de message à partir de celui-ci comportant un nombre multiple de secteurs de chiffres,
un moyen (50) au niveau dudit premier emplacement destiné à produire une première clé de session,
un second moyen de cryptage (55) couplé de façon à recevoir le nombre aléatoire de l'utili-

sateur et un secteur sélectionné du code d'authentification de message afin de crypter celui-ci avec la première clé de session conformément à une seconde combinaison logique de celle-ci afin de produire une première sortie codée (62),

un troisième moyen de cryptage (60) couplé de façon à recevoir le numéro d'identification personnel de l'utilisateur pour crypter celui-ci avec la première clé de session conformément à une troisième combinaison logique de celle-ci afin de produire une seconde sortie codée (64),
un moyen (29) destiné à transmettre les première et seconde sorties codées et un message et un numéro de séquence provenant du premier emplacement, vers l'emplacement suivant,

un moyen au niveau de l'emplacement suivant destiné à produire la première clé de session (clé de session key_1),

un premier moyen de décryptage (61) au niveau de l'emplacement suivant, couplé de façon à recevoir la première sortie codée transmise (68) et la première clé de session pour un décryptage conformément à ladite seconde combinaison logique afin de procurer le nombre aléatoire et le code d'authentification de message (65),

un second moyen de décryptage (70) au niveau de l'emplacement suivant, couplé de façon à recevoir la seconde sortie codée transmise et la première clé de session pour un décryptage conformément à la troisième combinaison logique de celle-ci afin de produire le numéro d'identification personnel de l'utilisateur (63),
un troisième moyen de cryptage (67) au niveau de l'emplacement suivant, couplé de façon à recevoir le message et le numéro de séquence transmis afin de coder ceux-ci conformément à ladite première combinaison logique ainsi que le numéro d'identification personnel décrypté (63) afin de produire un code d'authentification de message comportant un nombre multiple de secteurs de chiffres,

un moyen de comparaison (74) au niveau de l'emplacement suivant, couplé de façon à recevoir les secteurs sélectionnés correspondants du code d'authentification de message (65) élaboré par le décryptage dudit premier moyen de décryptage (61) et du code d'authentification de message formé par le cryptage dudit troisième moyen de cryptage (67) au niveau dudit emplacement suivant afin de produire une indication en sortie de la parité de ceux-ci, et
un moyen (76) au niveau de l'emplacement suivant, qui répond à ladite indication en sortie afin d'agir sur le message reçu en réponse à une comparaison favorable.

6. Dispositif selon la revendication 5, comprenant :

un moyen (80) au niveau de l'emplacement suivant qui répond à une comparaison défavorable pour la transmission vers le premier emplacement d'un secteur sélectionné (58) du nombre aléatoire.

5

7. Dispositif selon la revendication 5, comprenant :

un moyen au niveau de l'emplacement suivant destiné à produire une seconde clé de codage (clé de session key_2),

10

un premier moyen de cryptage (69) au niveau de l'emplacement suivant, couplé de façon à recevoir le code d'authentification de message et le nombre aléatoire décryptés destiné à coder ceux-ci avec la seconde clé de codage conformément à une quatrième combinaison logique, en réponse à ladite comparaison favorable afin de produire un troisième code de sortie pour une transmission vers un emplacement de destination,

15

20

un second moyen de cryptage (78) au niveau de l'emplacement suivant, couplé de façon à recevoir le numéro d'identification personnel décrypté afin de coder celui-ci avec la seconde clé de codage conformément à une cinquième combinaison logique, en réponse à ladite comparaison favorable afin de produire un quatrième code de sortie (82) pour une transmission vers un emplacement de destination,

25

30

un moyen au niveau de l'emplacement de destination, destiné à produire la seconde clé de codage (clé de session key_2),

un premier moyen de décryptage (92) au niveau de l'emplacement de destination, destiné à recevoir le troisième code de sortie (90) transmis depuis ledit emplacement suivant et la seconde clé de codage afin de décoder ceux-ci conformément à ladite quatrième combinaison logique afin de procurer le nombre aléatoire (94) et le code d'authentification de message (75),

35

40

un second moyen de décryptage (71) au niveau de l'emplacement de destination, destiné à recevoir le quatrième code de sortie transmis depuis ledit emplacement suivant et la seconde clé de codage (clé de session key_2) afin de décoder ceux-ci conformément à ladite cinquième combinaison logique afin de procurer le numéro d'identification personnel,

45

50

un moyen de cryptage (77) au niveau de l'emplacement de destination destiné à recevoir le message et le numéro de séquence en vue de coder ceux-ci ainsi que le numéro d'identification personnel décrypté conformément à la première combinaison logique afin de produire un code d'authentification de message comportant un nombre multiple de secteurs de chiffres,

55

un moyen (79) au niveau de l'emplacement de destination destiné à comparer des secteurs sélectionnés correspondants du code d'authentification de message crypté et du code d'authentification de message décrypté (75) afin de produire des indications en sortie de comparaisons favorable et défavorable,

un moyen (81) au niveau de l'emplacement de destination, qui répond à une indication en sortie favorable afin d'agir sur le message transmis et de transmettre un secteur sélectionné du nombre aléatoire vers ledit premier emplacement, et qui répond (83) à une comparaison défavorable afin de transmettre un autre secteur sélectionné du nombre aléatoire vers ledit premier emplacement, et

un moyen de comparateur (98) au niveau du premier emplacement, couplé de façon à recevoir les secteurs sélectionnés correspondants du nombre aléatoire en vue de procurer une indication en sortie (89, 91) de l'état de l'opération exécutée sur un message au niveau de l'emplacement de destination.

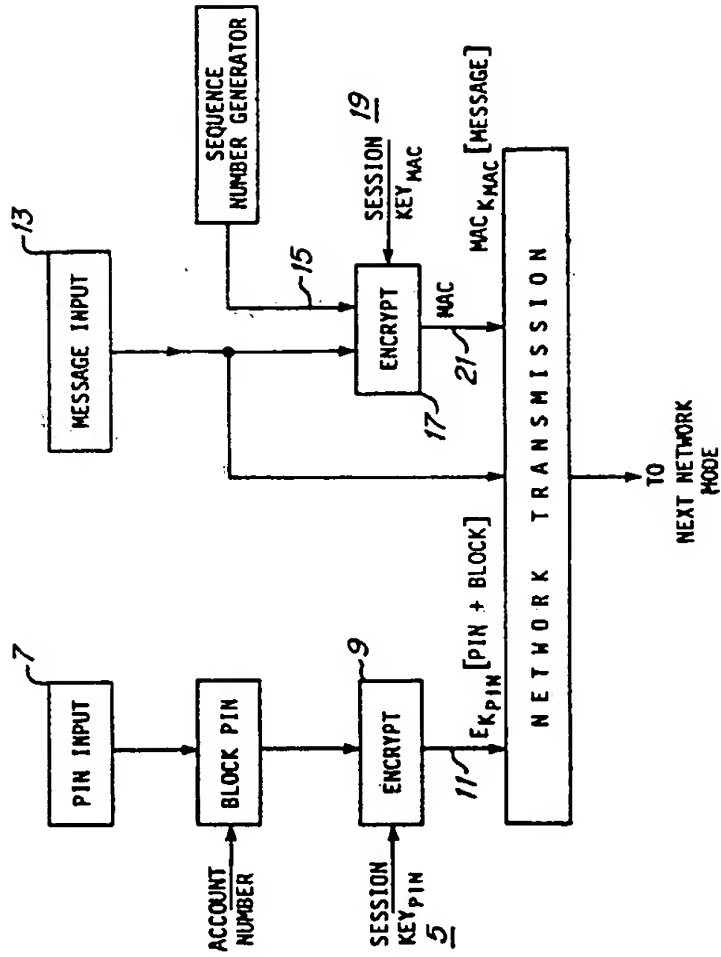


Figure 1
(PRIOR ART)

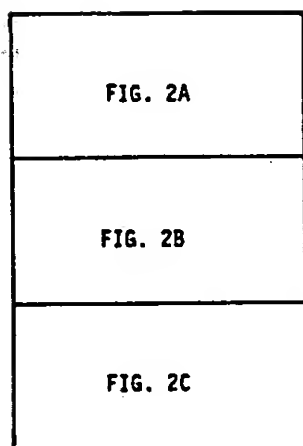


Figure 2

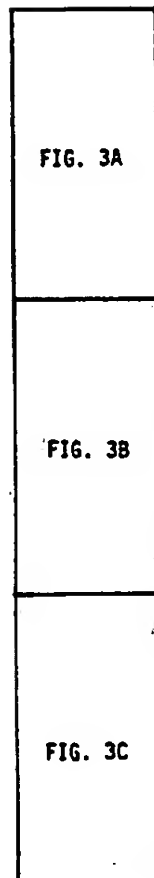


Figure 3

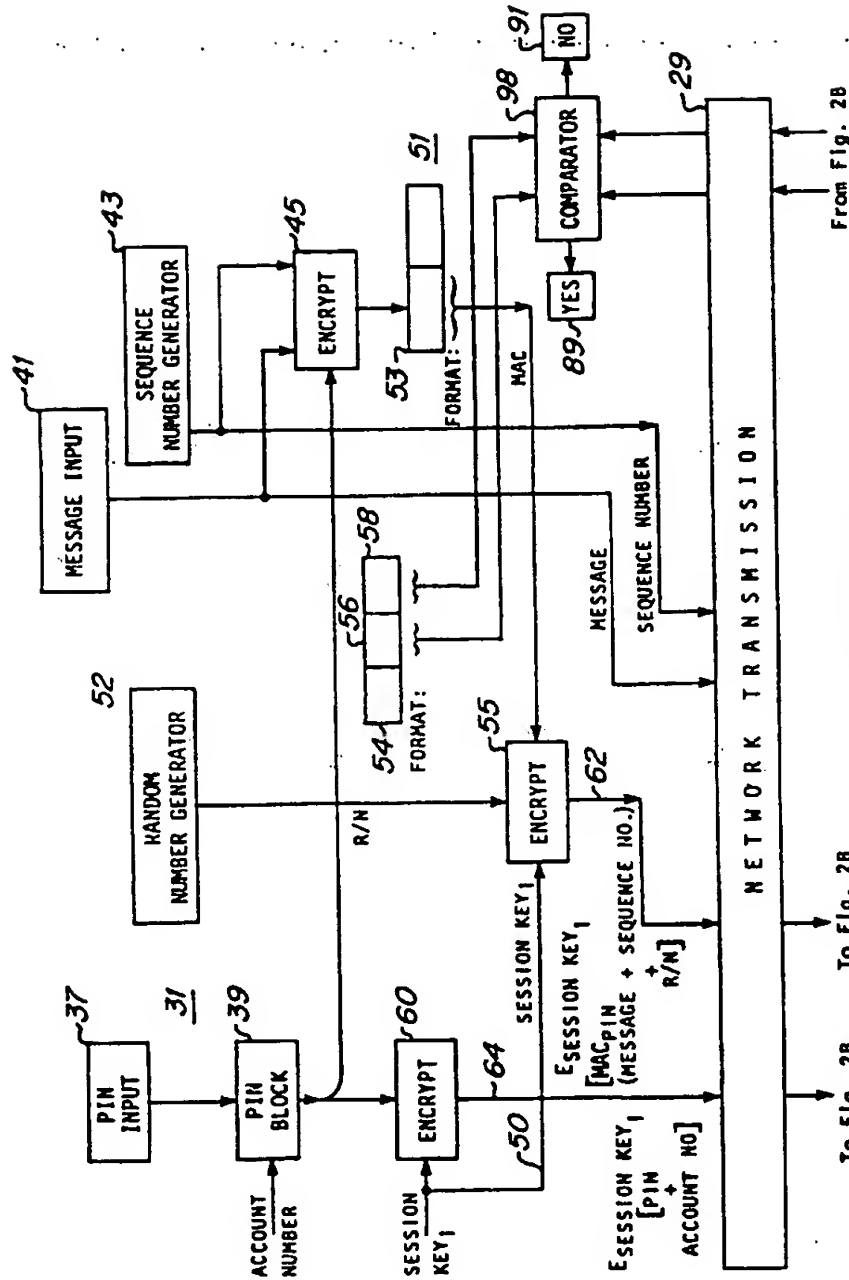


Figure 2A

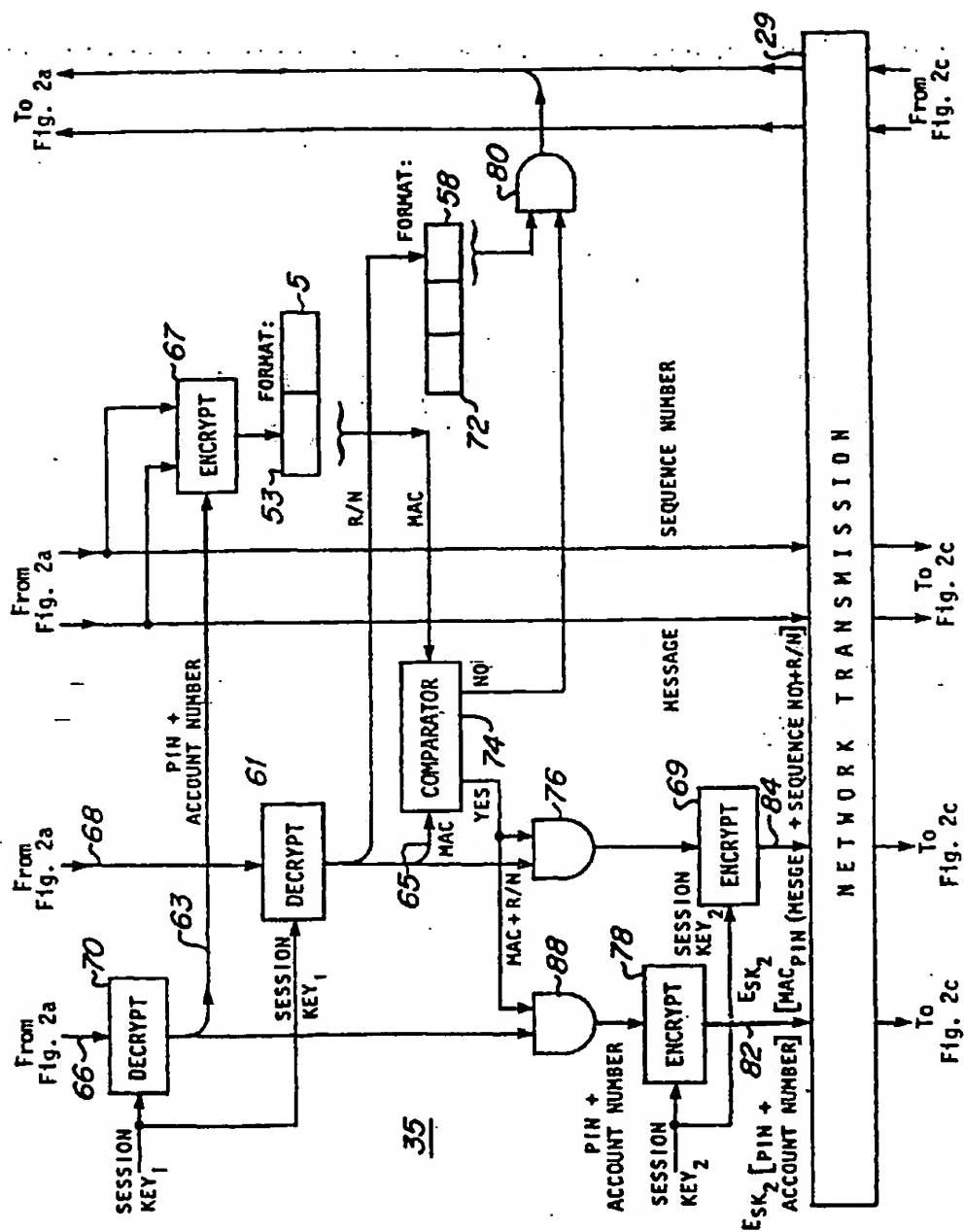
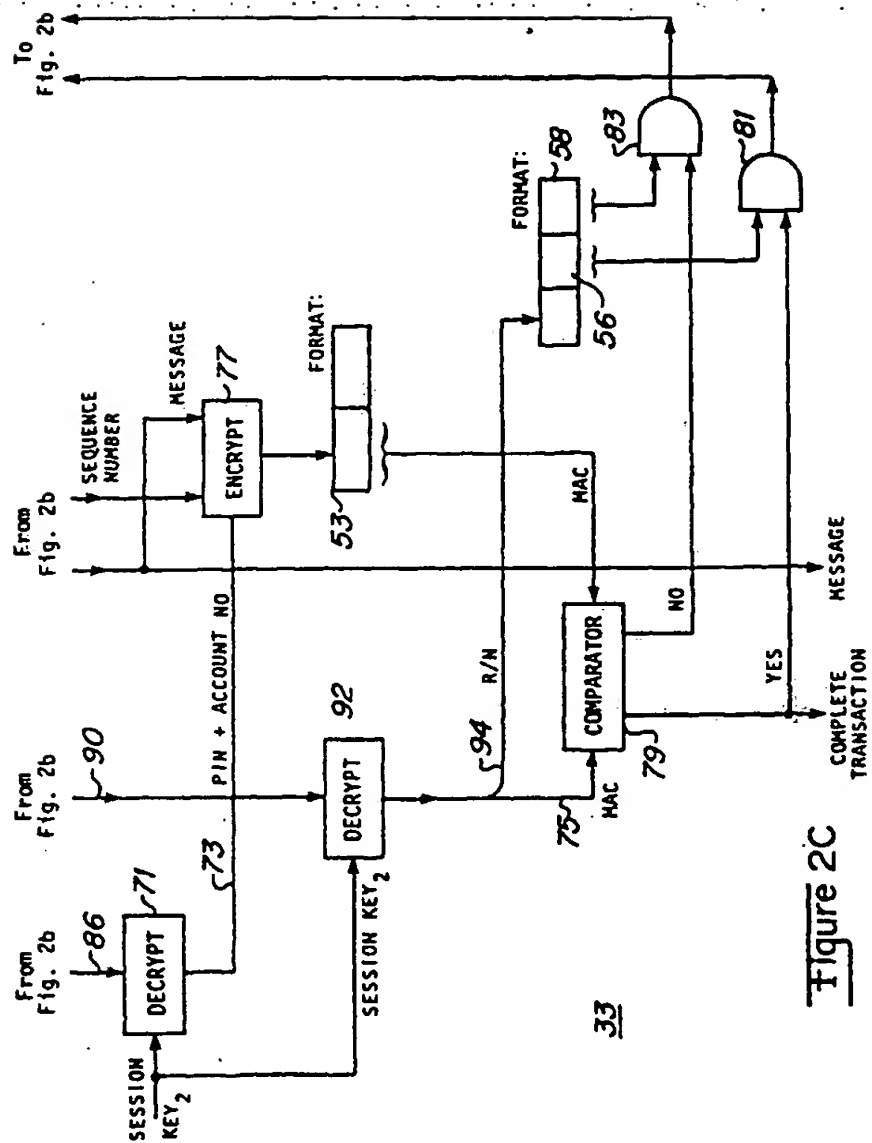


Figure 2B



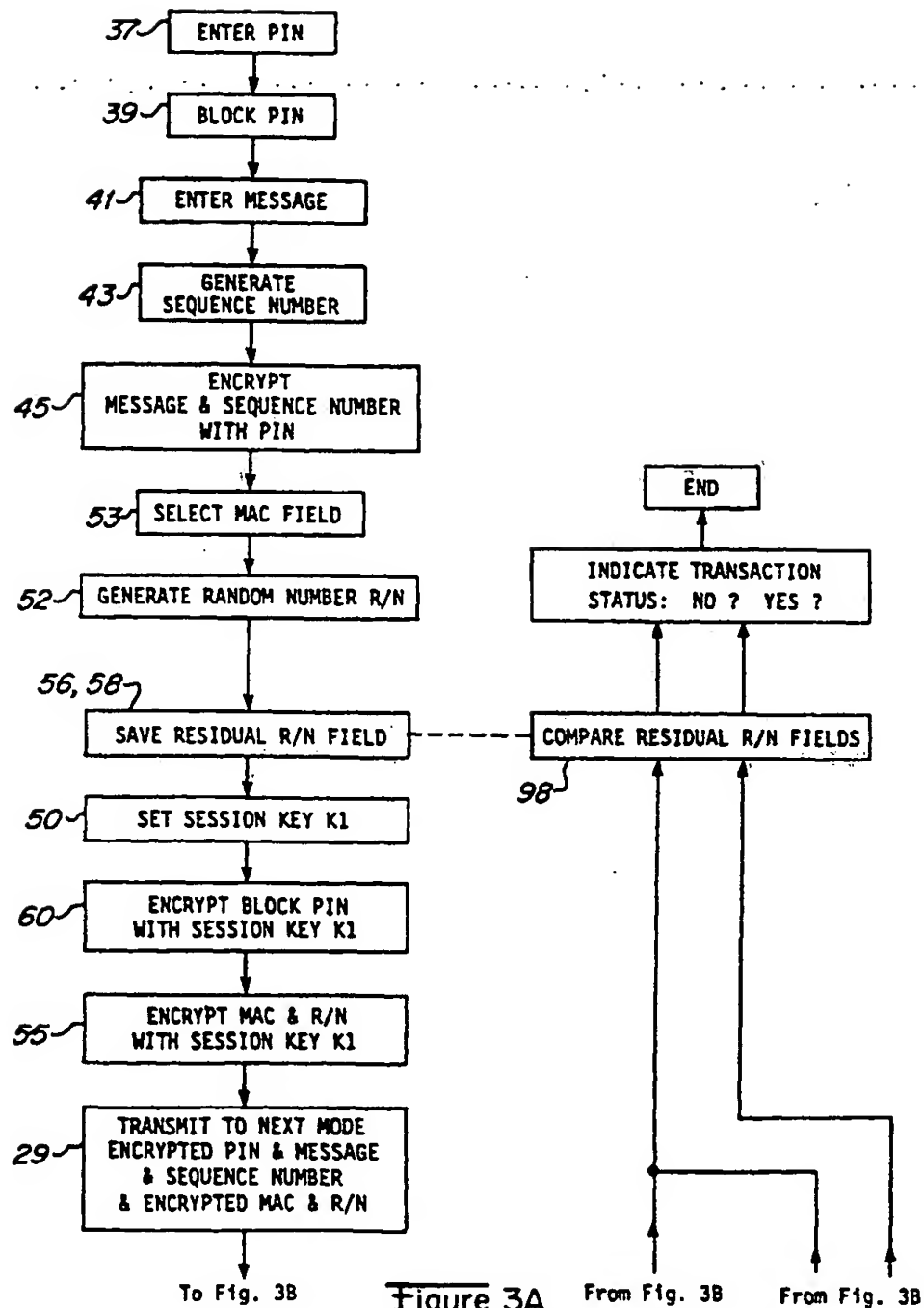
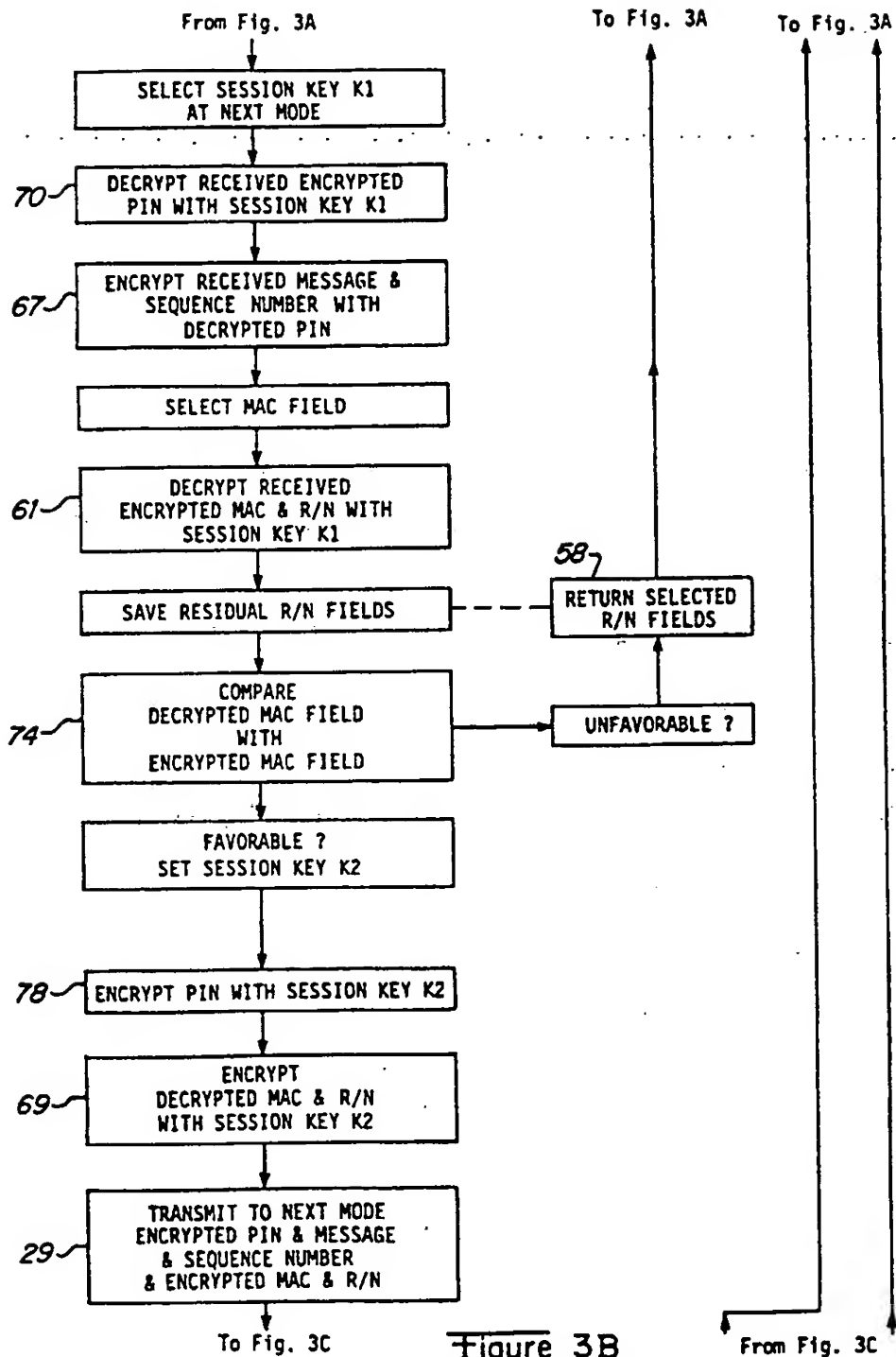


Figure 3A



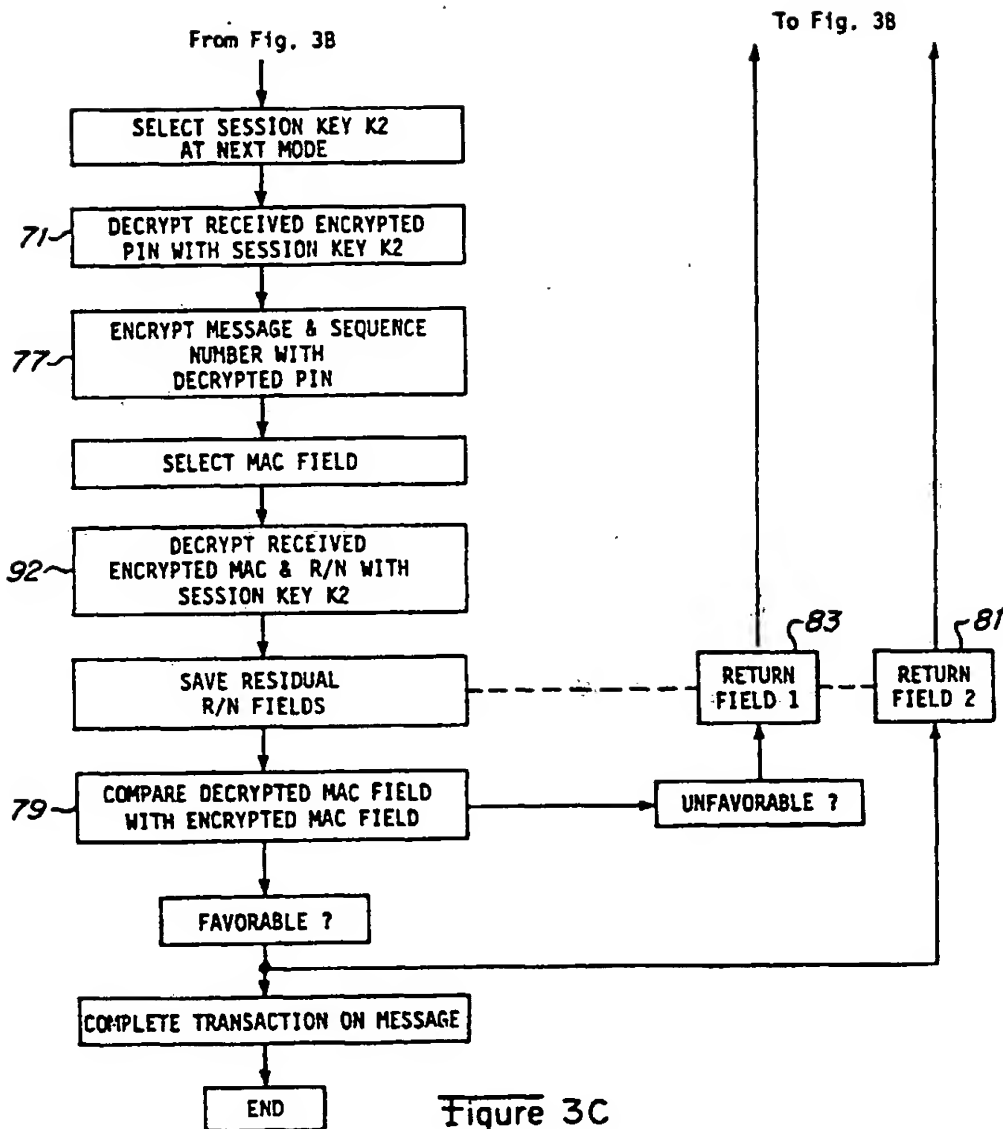


Figure 3C